

行業概覽

除另有說明外，本節所載資料均來自各種官方政府出版物、其他出版物以及本公司委託弗若斯特沙利文編製的市場研究報告。本公司相信，該等資料來自適當的來源，並已於摘錄及轉載該等資料時採取合理慎審態度。本公司並無理由相信該等資料在任何重大方面屬虛假或具有誤導性，或存在任何事實遺漏而導致有關資料在任何重大方面屬虛假或具有誤導性。本公司或其任何各自董事、高級職員或代表或參與本文件的任何其他人士並無獨立核實該等資料，亦未就其準確性或完整性發表任何聲明。

中國信息安全市場概覽

定義及分類

信息安全是一個涵蓋性術語，囊括所有為保護信息所做的工作，亦指在信息的生產、傳輸、處理和存儲過程中，保護信息免遭未經授權的訪問、破壞、篡改和洩露，確保信息的可用性、保密性、完整性和不可否認性，並保障信息系統的可靠性和可控性。具體而言，信息安全包含若干主要領域：網絡安全、數據安全及其他。網絡安全更側重於對計算資源和網絡環境的安全防護，而數據安全則著重於保護數據從生成到銷毀的整個生命週期，二者均屬於信息安全範疇。

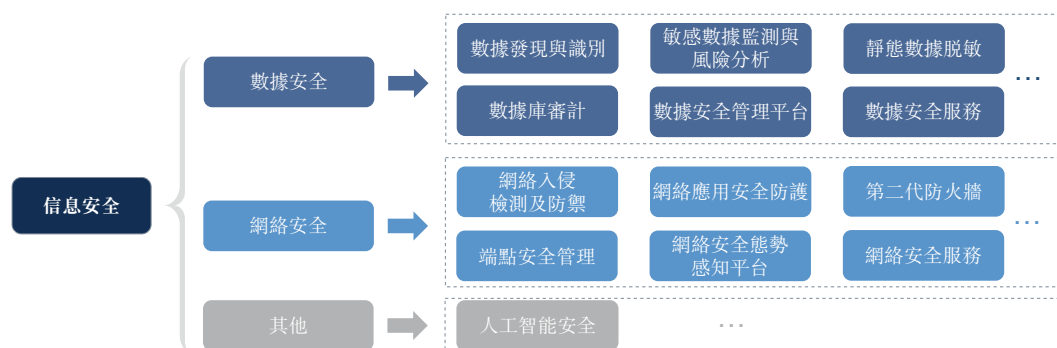


圖1.信息安全分類

資料來源：弗若斯特沙利文；市場參與者的官方網站；行業專家訪談

中國信息安全市場推動因素

技術：隨著技術的持續進步，特別是雲計算、大數據、人工智能和物聯網等新興技術的發展，對信息安全提出更高要求。這些技術的應用帶來新的安全挑戰，例如數據洩露、網絡攻擊等，同時也催生新的安全技術和解決方案。例如，人工智能技術正日益應用於網絡安全領域，它能夠幫助預測和識別潛在的安全威脅，並提升響應速度與準確性。

政策：政府日益重視信息安全，並出台一系列政策及法規以加強信息安全管理及保護。例如，中國的《網絡安全法》、《數據安全法》和《個人信息保護法》為網絡空間的安全提供法律支持。這些政策的實施促進了信息安全產品與服務需求的增長，並推動該行業的標準化與市場化進程。

事件：近年來，網絡釣魚、安全漏洞、惡意程序、網頁篡改、網絡後門、DDoS攻擊等安全事件頻發，不僅給受影響的組織帶來直接損失，亦提升全社會對信息安全的意識和需求。例如，「網絡防護行動」是國家應對網絡安全問題的重要部署之一。

行業概覽

中國信息安全市場產業鏈

隨著中國信息安全行業的發展，產業鏈已逐漸趨於完善。產業鏈上游主要為基礎軟硬件供應商，例如芯片、內存、存儲設備、服務器及工業電腦的硬件供應商，其為信息安全提供所需的實體基礎設施；以及提供操作系統、數據庫及中間件的軟件供應商，其為信息安全系統提供基礎技術及底層運行環境。

產業鏈中游由信息安全產品及服務提供商組成，按產品類型可分為標準信息安全產品、信息安全平台及信息安全服務提供商。具體而言，各產品類別可進一步細分為兩大類：網絡安全及數據安全。例如，標準信息安全產品可細分為標準網絡安全產品及標準數據安全產品。

產業鏈下游由應用領域及終端用戶組成，包括電信、政府、能源及電力、金融、工業製造及醫療保健，該等領域為信息安全的需求來源。

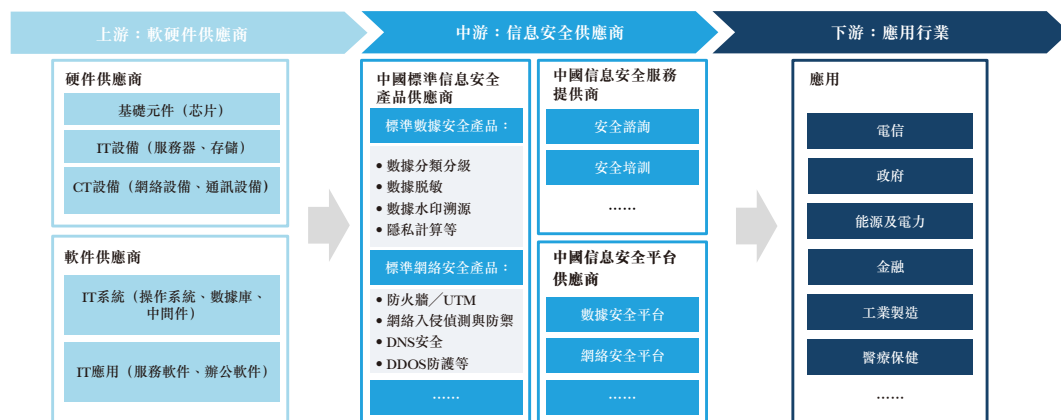


圖2.信息安全市場產業鏈

資料來源：弗若斯特沙利文；行業專家訪談

中國信息安全市場規模

中國信息安全市場規模已從2021年的人民幣732億元增長至2025年的人民幣1,057億元，複合年增長率達9.6%。該增長主要源於政策合規要求和頻發的安全事件，這些因素迫使企業加速對信息安全的投資。

預期市場規模將由2026年的人民幣1,154億元增加至2030年的人民幣1,727億元，複合年增長率10.6%。人工智能技術的融合催生了對「AI+安全」解決方案的激增需求，而人工智能安全、車聯網(IoV)、物聯網(IoT)及雲安全等新興領域的加速需求釋放，共同構成市場持續擴張的核心驅動力。

從信息安全市場中游參與者的具體角色來看，該等參與者大致可分為兩類：(i) 傳統互聯網/ICT製造商，例如華為、阿里巴巴、騰訊及中國電信等；(ii) 專業安全製造商，例如奇安信、觀安信息、安恒信息、啟明星辰等。

對信息安全市場參與者的上述分類主要源於其業務定位及增長策略的顯著差異：前者通常將安全視為雲端、網絡或數字化解決方案的輔助能力，其安全收入分散於整體ICT業務中；然而，後者將網絡安全及數據安全作為其核心業務，專注於攻防演練、數據治理及合規營運等深度場景。因此，其業務表現更能直接反映行業實際需求及技術進步。因此，在進行市場分析時，有必要對專業安全供應商群體進行單獨分析。

行業概覽

中國信息安全專業安全供應商細分市場規模從2021年的人民幣283億元增長至2025年的人民幣390億元，複合年增長率達8.4%。這種增長主要源於專業安全供應商不斷深化技術專長、加速場景滲透，以及政策合規要求和安全事件的推動。

預期市場規模將由2026年的人民幣421億元增加至2030年的人民幣650億元，複合年增長率為11.5%。專業安全供應商專注於尖端領域以快速應對新興威脅，其在垂直行業的深厚專業知識使其能夠精準解決特定行業的痛點，為進一步拓展市場鋪平道路。

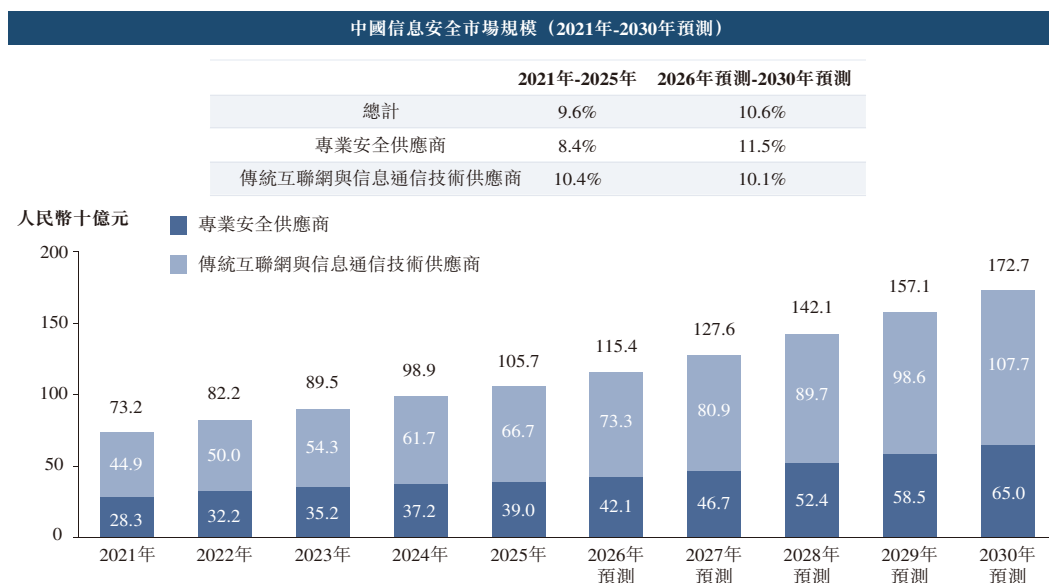


圖3. 中國信息安全市場規模

資料來源：弗若斯特沙利文；行業專家訪談

中國信息安全市場的未來趨勢

數字技術的大規模應用催生新的安全漏洞。隨著人工智能、雲計算和大數據等數字技術的廣泛商業應用，傳統安全邊界正受到衝擊。人工智能系統可能存在內生性安全問題，例如大型模型中的漏洞和算法偏見。跨域調度和共享計算能力資源可能帶來數據洩露和計算能力濫用的風險。這些新場景提出了傳統網絡/數據安全措施無法應對的安全需求，這將推動新興安全領域的開發。

人工智能安全將成為數字時代的關鍵趨勢。人工智能安全需要在人工智能創新與風險管理之間取得平衡：從技術層面看，人工智能不僅能增強威脅檢測能力，同時也面臨數據投毒等風險。諸如對抗性訓練等防護技術正加速其應用進程。在管治方面，許多國家已出合法規和標準，明確規定了高風險人工智能評估的要求。在產品層面，新興且不斷演進的解決方案—例如基於「主動自主防禦、全生命週期保護、以模型對抗模型」原則運作的安全代理—有望解決人工智能安全領域的痛點。在應用層面，它深入金融、工業等領域，並與網絡安全、數據安全深度融合，形成一體化防護解決方案。

物聯網與安全要求的深度綁定。物聯網的普及打破了傳統的安全邊界。物聯網設備的廣泛普及顯著擴大了攻擊面。曾經孤立的設備風險已透過網絡連接演變為系統性安全風險，牽動公共安全與經濟穩定，並推動物聯網安全從邊緣需求升級為核心必需。政策合規約束與專屬技術創新（如輕量級加密和可信認證）進一步增強其技

行業概覽

術獨立性，而與新興技術的融合構建了全鏈條防護生態體系，使其成為保障數字化轉型、引領信息安全市場發展的關鍵方向。

對新興安全情境加強監管約束。《數據安全法》和《個人信息保護法》等法規對人工智能訓練數據的隱私保護以及在計算能力共享過程中數據流的合規性提出明確要求。《物聯網新型基礎設施建設三年行動計劃》等文件進一步明確了對設備身份驗證、加密通訊及安全固件升級等環節的強制性要求。尋求部署人工智能應用或開展跨域計算能力協作的企業必須滿足這些合規標準。這種嚴格的約束將直接促進對新興安全市場的投資。

平台驅動的產品、運營與服務一體化，已成為安全行業發展的關鍵路徑。數字化轉型推動安全威脅呈現出更複雜、更多元的態勢，單一產品防護已不足以應對整體風險。基於平台的開發因此已成為行業必然趨勢。產品、平台與服務的集成化模型圍繞平台核心整合全面的安全能力。專業安全服務作為銜接環節，涵蓋安全諮詢及應急響應等端對端服務。這些服務彌補了企業安全團隊的不足，並解決了「重部署、輕運維」的痛點。專業產品奠定基礎，定制化服務則確保效能與動態調適能力。此模式不僅滿足合規要求，更推動防禦體系從被動防禦轉向主動運營，助力構建高效的安全生態，已成為產業高品質發展的關鍵驅動力。

中國數據安全市場概覽

定義及分類

數據安全指通過採取必要措施，確保數據處於有效保護與合法利用的狀態，以及保障持續安全狀態的能力。具體而言，數據安全是以數據為中心的安全體系，涵蓋數據採集、傳輸、儲存、處理(使用)、交換(共享)與銷毀等全生命週期環節，聚焦從數據生成至銷毀全過程的防護，強調數據所有權、管轄權、隱私權等。隨著信息化水平的不斷提高及數據時代的到來，數據的存儲節點與區域日益複雜，數據流量呈現指數級增長，使用方式亦日益多樣化。原有的防護方式已無法滿足當前的安全需求，數據安全已成為獨立的安全體系。

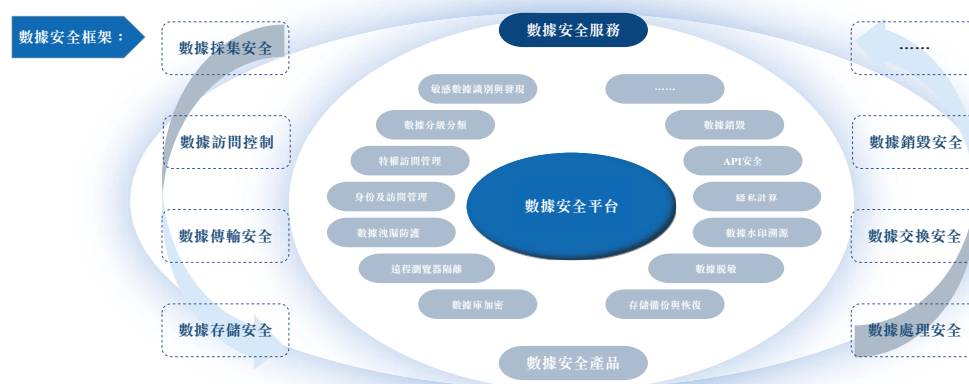


圖4.數據安全市場框架

資料來源：弗若斯特沙利文；市場參與者的官方網站；行業專家訪談

行業概覽

數據安全平台的定義

數據安全平台是一個涵蓋全生命週期及所有場景的綜合安全系統，涵蓋數據從生成、存儲、傳輸、使用到銷毀的整個過程，提供統一的數據安全保護、治理與合規能力。其核心目標是實現數據的「可知、可控、可防、可溯」，並透過統一架構整合數據洩露防護、數據加密、訪問控制、風險監測及合規審計等多個子系統。其特點是：

- (i) 這是企業級數據安全治理的頂級平台。
- (ii) 它包括數據安全管理平台、安全數據中心、數據資產與風險評估平台等。
- (iii) 提供跨部門和系統的統一安全視圖及政策聯繫。

中國數據安全市場驅動因素

外部因素：合規要求，穩定增長

數據安全監管趨勢：監管機構對數據安全的監督與關注逐年加強，主要由中央政府與工業和信息化部牽頭推進。電信、政府、能源電力、金融及製造行業是數據安全監管更為嚴格的行業。

內部因素：內在價值，需求激活

數據量的快速增長激發了對數據安全更高的關注度：根據弗若斯特沙利文的統計數據，中國數據總量已從2019年的9.8ZB激增至2025年的52.3ZB。隨著數據量的增加，隱藏在數據背後可挖掘的信息變得日益豐富。數據已從單純的輔助性資源，演變為政府與企業發展的核心戰略資產。其在決策支持、效率提升及業務創新等方面的價值日益凸顯。在此背景下，政府與企業愈發重視數據的價值，並積極探索如何在安全可控的環境下充分挖掘數據潛能、最大化釋放其價值。

數據洩露成本的攀升推動了企業數據安全需求。2025年全球數據洩露事件的平均成本高達數百萬美元，且呈快速增長態勢。由於數據敏感性，醫療保健、金融服務和新能源汽車等行業每年因數據洩露造成的損失都在持續攀升。數據洩露的高昂代價使企業深刻認識到數據安全的重要性，促使管理層更加重視數據安全防護工作，將數據安全納入企業核心戰略，加大數據安全投入，並積極採取多種措施保護企業數據資產。與此同時，為降低數據洩露風險及潛在損失，企業對數據安全產品與服務的採購需求顯著增加。此外，面對數據洩露成本的持續攀升，企業探索並應用新型安全技術與創新解決方案的動力更強，例如在數據安全領域應用人工智能、機器學習、區塊鏈等技術。

大數據與人工智能模型的發展帶來機遇與需求。大數據與人工智能模型的發展為數據安全帶來諸多機遇，例如提升監測與防護能力、優化數據管理、提供治理決策支持、推動技術創新以及增強用戶安全意識。與此同時，這一發展也催生了對數據安

行業概覽

全的新需求，涵蓋數據生命週期保護、模型可靠性保障、隱私增強、改進協作共享機制以及專業人才和技術支持等多個方面。

中國數據安全市場行業痛點

賬戶、權限與API成為數據保護中的薄弱環節：其中特權賬戶已成為最嚴重的「安全漏洞」之一，權限問題在新IT環境中演變為嚴峻的安全挑戰。API防護長期被忽視，已成為數據安全面臨的最大風險暴露點。

數據安全狀態持續防護的實施難點：如今，數據呈現分佈廣泛、規模龐大、資產分散以及跨複雜場景快速流轉的特徵，為安全防護帶來前所未有的困難。同時，多樣化的數據存取來源使建立統一的聯防聯控機制變得複雜。傳統以疊加方式部署離散數據安全工具的方法僅能以碎片化方式應對風險，無法實現全面及系統的聯防聯控。

傳統防護系統失效與攻擊手段升級：大多數企業仍依賴傳統防火牆和入侵檢測系統，難以識別透過供應鏈植入的惡意代碼，極易導致客戶交易數據洩露。生成式人工智能被用於製造高度逼真的釣魚郵件，從而提升攻擊成功率，而僅有少數生成式人工智能項目採取充分的安全措施。

數據治理體系的結構性缺陷：合規要求、技術框架與實際業務需求之間存在錯位。具體而言，與數據跨境流動相關的合規成本依然高企，而內部治理機制未能有效緩解供應鏈風險及內部威脅。同時，隱私計算及數據匿名化等技術的效能及成效仍不足以滿足實際業務需求。

中國數據安全市場細分

中國數據安全市場規模

從2021年到2025年，中國數據安全市場規模從人民幣186億元躍升至人民幣290億元，複合年增長率達11.7%。

從2026年到2030年，市場規模預計將由人民幣323億元增長至人民幣509億元，複合年增長率為12.1%。市場增長的驅動因素將日益多元化，主要由人工智能、隱私保護計算及量子密碼學等技術的融合，以及金融、車聯網(IoV)及物聯網(IoT)等行業對數據安全日益迅速增長的需求所驅動。

而中國數據安全專業安全供應商細分市場規模由2021年的人民幣53億元躍升至2025年的人民幣78億元，複合年增長率達10.1%。推動這一變革的主要動力，是行業數字化轉型引發的場景化需求爆發式增長，與各供應商的技術創新共同驅動產品能力實現飛躍。從2026年到2030年，市場規模預計將由人民幣85億元增長至人民幣137億元，複合年增長率為12.6%。展望未來，「人工智能與數據安全」的融合將推動在整個數據生命週期中實現準確高效的保護。與此同時，隨著在電信、政府及金融等垂直行業內數據安全的要求繼續演變，這將推動對特定場景及定製化產品及服務的需求日益增長。

行業概覽

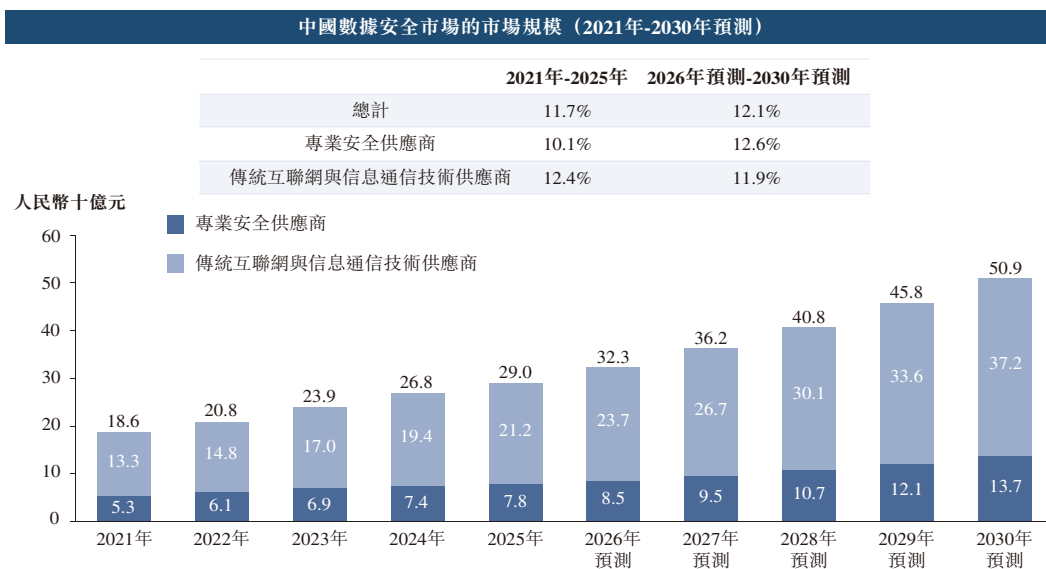


圖5. 中國數據安全市場規模

資料來源：弗若斯特沙利文；行業專家訪談

中國數據安全平台市場規模

在市場平台化、智能化和場景化應用的明顯趨勢下，數據安全產品亟需從「單模塊」解決方案升級為涵蓋數據「發現、治理、保護及運營」的一體化平台，這推動了數據安全平台市場的蓬勃發展。

中國數據安全平台市場規模從2021年的人民幣45億元增長至2025年的人民幣76億元，複合年增長率為13.9%。並預計到2030年將增長至人民幣154億元，自2026年至2030年的複合年增長率為15.3%。

從數據安全專業安全供應商細分市場層面來看，市場規模已由人民幣9億元增長至人民幣15億元，2021年至2025年的複合年增長率為13.9%。預計到2030年將增長至人民幣31億元，2026年至2030年的複合年增長率為15.5%，展現出強勁的增長潛力。

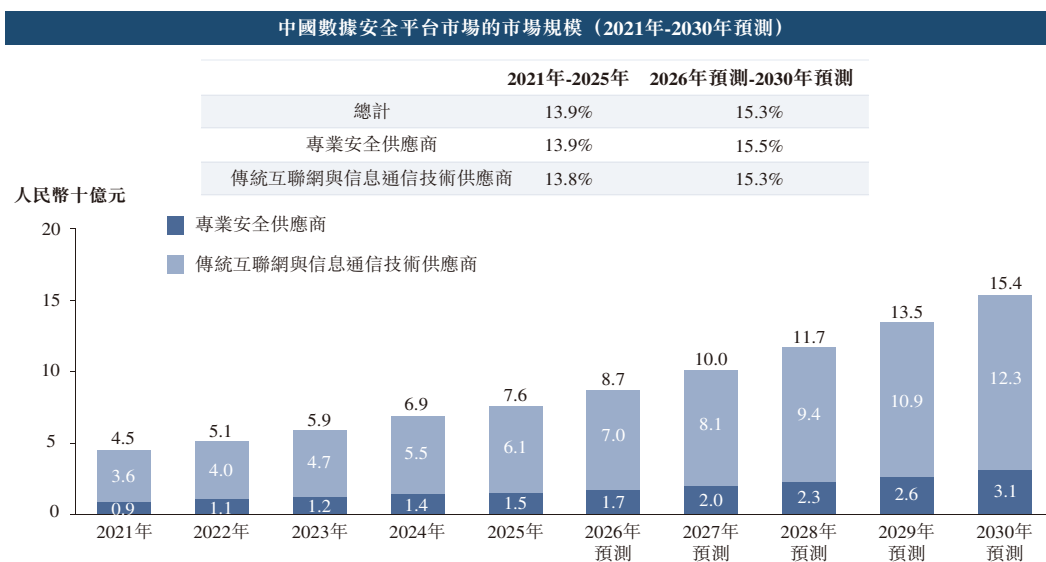


圖6. 中國數據安全平台市場規模

資料來源：弗若斯特沙利文；行業專家訪談

行業概覽

中國數據安全市場的未來趨勢

數據安全的整合與平台化

數據安全日益複雜，導致不同數據安全功能逐漸整合。當前數據安全建設現狀不僅源於對數據安全的重視不足或投入不足，更常見的是：即便部分企業已為數據安全投入充足預算，由於數據安全技術的複雜性，以及從不同安全廠商採購各類安全產品且由不同團隊管理，導致前期投入的安全預算未能取得理想成效。當前數據安全技術複雜性的增長速度遠超安全廠商整合各類新興技術的能力，導致用戶端應用數據安全技術的難度持續攀升。數據安全平台將現有的獨立數據安全技術與功能整合為統一平台，為用戶提供跨數據類型、存儲孤島及生態系統的數據安全服務，從而實現更簡潔、更一致的端到端數據安全防護。

「數據安全+人工智能」已成為重要趨勢

透過運用人工智能技術，能夠快速識別並從海量合規政策、威脅情報、行業動態及最佳實踐中學習模式，挖掘並分析有價值的信息，開展智能決策分析，從而為數據安全提供精準的策略與方案。透過運用自動化工具和方法，可提升數據安全評估中多個環節的效率與準確性，包括問卷調查、人員訪談、文件審查、配置驗證、現場核查、技術測試、專家分析及報告編製等環節，從而幫助企業更有效地識別和應對數據安全風險。在數據安全策略方面，人工智能能夠根據數據的敏感程度和使用場景自動調整數據訪問控制與加密策略，從而保障數據安全。

隱私計算已成為當前最熱門的話題

近年來，在數據安全領域最具工業應用前景的技術當屬隱私計算。隱私計算能夠在完成計算任務的同時，對數據計算過程及結果實現隱私保護，參與者在整個計算過程中除計算結果外無法獲取其他額外信息。隱私計算並非單一技術，而是由多種技術組成的技術系統。關鍵技術包括多方計算、聯邦學習、可驗證去標識化、保密計算、同態加密等。不同的技術路線會顯著影響產品的使用場景、功能及性能表現。

中國網絡安全市場概覽

定義及分類

網絡安全是指透過技術、管理和法律手段保護網絡系統(包括硬件、軟件、服務等)免受攻擊、入侵、破壞和非法使用，確保網絡的可用性、完整性和保密性。網絡安全具體涵蓋網絡空間與物理空間的安全，包括網絡系統的運行安全、網絡信息的內容安全、網絡傳輸的安全以及網絡實體的物理資產安全：

- (i) 從行業角度來看，網絡安全的下游市場可分為運營商、金融、政府、工業製造、醫療、教育等領域。
- (ii) 從產品形態角度來看，網絡安全市場可分為標準網絡安全產品市場、網絡安全平台市場和網絡安全服務市場。

行業概覽

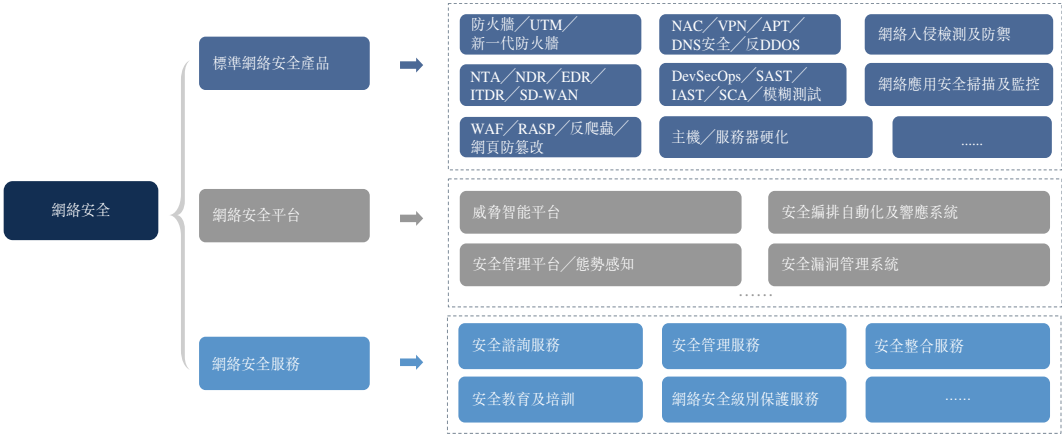


圖 7. 網絡安全分類

資料來源：弗若斯特沙利文；市場參與者的官方網站；行業專家訪談

中國網絡安全市場細分

中國網絡安全市場規模

自2021年以來，中國的網絡安全市場在政策引導、技術升級和行業需求推動下呈現顯著增長態勢。市場規模從2021年的人民幣546億元增加至2025年的人民幣767億元，複合年增長率為8.9%。預計到2030年將增至人民幣1,219億元，從2026年到2030年的複合年增長率為10.0%。

而中國網絡安全市場(尤其是專業安全供應商細分市場)由2021年的人民幣230億元增長至2025年的人民幣312億元，複合年增長率達8.0%。此增長主要受關鍵信息基礎設施領域(包括政府、企業、金融及能源)對合規性的強勁需求所驅動，加上數字化轉型背景下企業安全意識的全面提升，共同推動專業網絡安全產品及服務採購的持續擴大。預計到2030年，該市場將達到人民幣514億元，從2026年到2030年的複合年增長率為11.2%。專業安全供應商在高級攻防、安全治理及營運等領域所建立的技術壁壘，將使其在對合規性與安全標準要求較高的場景中保持核心競爭優勢，從而支持市場穩步增長。

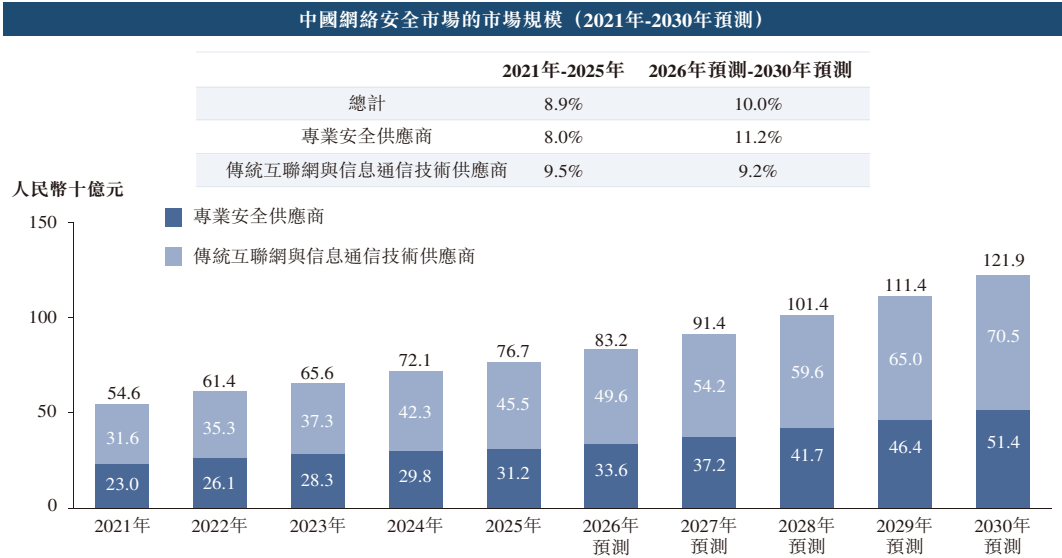


圖 8. 中國網絡安全市場規模

資料來源：弗若斯特沙利文；行業專家訪談

行業概覽

中國網絡安全平台市場規模

網絡安全平台為一項整合多種安全技術、產品及服務的綜合安全解決方案，涵蓋威脅情報平台、安全編排自動化及響應平台、態勢感知平台及其他。通過建立「監控、分析、響應及改進」的閉環系統，其協助企業發展常態化及系統化的安全營運能力。

中國網絡安全平台市場由2021年的人民幣123億元增長至2025年的人民幣198億元，複合年增長率達12.6%。預計到2030年將增長至人民幣351億元，2026年至2030年的複合年增長率為12.4%。

作為網絡安全市場的重要領域，專業安全供應商更聚焦於網絡安全攻防技術、安全營運及治理等深度場景。其更能反映行業實際安全需求及技術發展方向。中國網絡安全平台專業安全供應商細分市場由2021年的人民幣39億元增長至2025年的人民幣59億元，複合年增長率達10.7%。預計到2030年將增長至人民幣103億元，2026年至2030年的複合年增長率為12.5%。

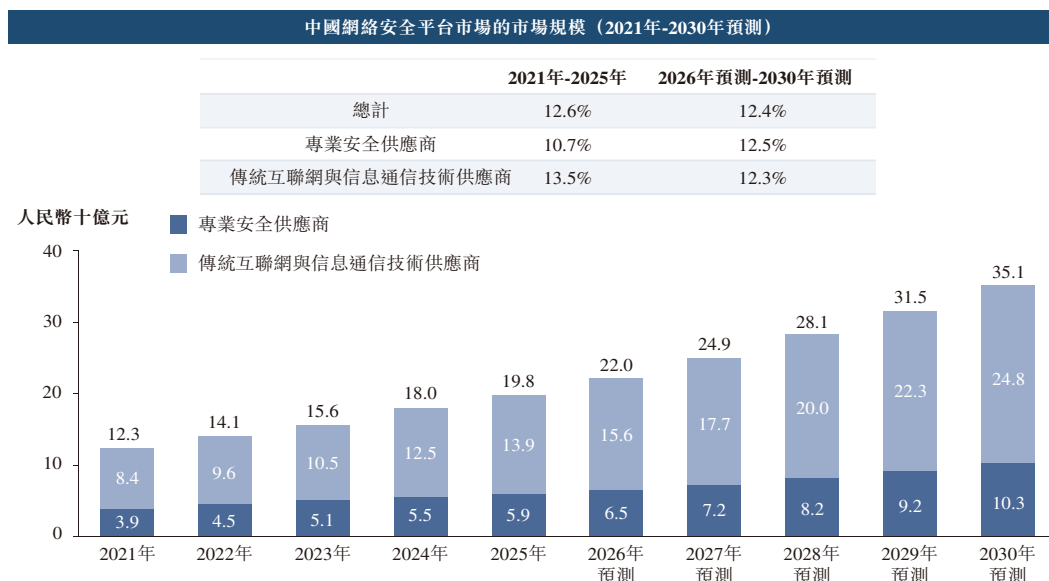


圖9. 中國網絡安全平台市場規模

資料來源：弗若斯特沙利文；行業專家訪談

網絡安全市場的未來趨勢

人工智能深度赋能網絡安全防禦系統：人工智能在網絡安全領域的應用將變得更加廣泛和深入。人工智能技術已從輔助工具升級為防禦核心。透過機器學習構建的行為基準，實時識別異常流量和釣魚郵件等威脅。未來，人工智能將主導網絡安全的攻防態勢，推動安全產品的智能化發展，實現對網絡威脅的自動監測、分析與響應。

零信任架構及身份優先：隨著邊界防禦的失效，零信任已成為主流安全策略。組織傾向於遵循「永不信任，始終驗證」的原則，嚴格控制資源訪問權限，並持續監控行為模式。未來，構建兼容多種產品的集成身份驗證工具與服務至關重要。持續的多因素認證(MFA)、行為分析與最低權限原則將與人工智能威脅檢測深度融合，實現更動態的訪問控制。

朝向平台化與服務化演進。數字化轉型催生出大規模、跨領域的複雜網絡威脅，傳統單點防禦難以適應全域動態風險。平台化已成為建構層次化防禦體系的關鍵路徑—透過安全運營與態勢感知平台整合多元安全能力，打破產品孤島，實現全局風險

行業概覽

可視可控。同時，安全服務正從被動事件響應轉向主動化、常態化運營。諮詢、託管服務、合規評估等綜合服務，不僅彌補企業能力缺口，更能動態適配風險變化，成為實現平台效能的關鍵支撐。

競爭格局

中國信息安全供應商分析

信息安全市場競爭激烈，參與者眾多。它們主要可分為兩類。一類由傳統互聯網與信息通信技術供應商組成，例如華為、阿里巴巴和騰訊。這些傳統供應商依託雲、網、端等基礎設施佈局，在網絡安全和數據安全領域形成了獨特的競爭力。

另一類是專業安全供應商，包括專業網絡安全供應商以及專業數據安全供應商，例如奇安信、觀安信息、安恒信息、啟明星辰等。這些專業安全供應商專注於技術深度、垂直場景和快速響應，建立防禦壁壘並迅速擴大市場份額。

專業安全供應商是信息安全市場中專業知識的核心底座。致力於提升安全能力，他們在攻防技術領域積累了深厚的專業知識，並持續推動創新發展。他們專注於尖端領域，迅速應對新興威脅並構建高效防護系統，成為安全生態系統中至關重要的參與者。

中國信息安全供應商排名(按專業安全供應商劃分)

2025年，中國信息安全市場規模(按競爭對手收入計算)達到人民幣1,057億元。其中，專業安全供應商佔比36.9%，市場規模達人民幣390億元。在2025年，根據收入統計數據，該細分市場的前五大領先企業分別為公司A、公司B、公司C、公司D及公司E，合計佔據39.3%的市場份額。在專業安全供應商中，本公司位列第13名，市場份額為1.8%。

中國信息安全市場在數字化轉型和網絡威脅加劇的背景下蓬勃發展。在監管要求(如《網絡安全法》)和數據安全、人工智能安全及物聯網安全需求激增的推動下，該市場正穩步擴張。企業競相創新，塑造出支撐產業安全數字化演進的動態格局，昭示著中國信息安全領域蘊藏著非凡的增長潛力。作為專業安全供應商，本公司位列其中第13位，彰顯其雄厚的技術實力與市場適應能力。

排名	公司	市場份額(按收入計)
1	公司A	11.2%
2	公司B	9.1%
3	公司C	6.5%
4	公司D	6.5%
5	公司E	5.9%
6	公司F	5.8%
7	公司G	5.5%
8	公司H	3.6%
9	公司I	3.1%
10	公司J	2.3%
11	公司K	2.1%
12	公司L	1.8%
13	本公司	1.8%
14	公司M	1.4%
15	公司N	1.4%
其他		31.7%
總計		100%

圖 10. 2025 年信息安全供應商收入排名前 15 位(中國，按專業安全供應商劃分)

資料來源：弗若斯特沙利文；各市場參與者的年報；行業專家訪談

行業概覽

附註：公司A成立於2014年，總部位於北京，於上海證券交易所上市。該公司專注於向政府及企業用戶提供新一代網絡安全產品與服務。

公司B成立於2000年，總部位於深圳，於深圳證券交易所上市。該公司專注於為企業級網絡安全、雲計算及物聯網領域提供創新產品與服務。

公司C成立於1985年，總部位於汕頭，於深圳證券交易所上市。該公司提供完整的網絡安全與智能運算雲產品、服務及整合解決方案。

公司D成立於2000年，總部位於北京，於深圳證券交易所上市。該公司是一家專注於安全領域的創新企業，提供涵蓋基礎設施安全、數據安全、雲安全等的全方位安全產品與服務。

公司E成立於1996年，總部位於北京，於深圳證券交易所上市。該公司專注於網絡安全產品、服務及解決方案，客戶涵蓋政府、電信、金融等領域。

公司F成立於1998年，總部位於四川，於深圳證券交易所上市。該公司專注於信息安全領域，業務涵蓋網絡安全、數據安全等場景。

公司G成立於2007年，總部位於杭州，於上海證券交易所上市。該公司主要從事網絡與信息安全軟件開發、安全諮詢服務，以及信息安全設備的製造與銷售。

公司H成立於2014年，總部位於南京，於上海證券交易所上市。作為一家專注於安全與數字智能的企業，其業務聚焦於雲安全與終端安全領域。

公司I成立於2008年，總部位於杭州，於2019年在深圳證券交易所上市。該公司是重要的信息安全廠商之一，專注於網絡安全及應用交付。

公司J成立於2011年，總部位於蘇州，於上海證券交易所上市。該公司專精於網絡安全，提供包括邊界安全、雲安全、數據安全等產品與服務。

公司K成立於2001年，總部位於北京，於2016年在深圳證券交易所上市。該公司是專注於網絡安全及電子認證服務的企業。

公司L成立於2002年，總部位於濟南，於2017年在深圳證券交易所上市。該公司是網絡安全及保密安全產品研發與整體解決方案的領先提供商。

公司M成立於2011年，總部位於北京，於2019年在上海證券交易所上市。該公司專注於網絡安全領域的核心技術與底層平台的研發、銷售及服務。

公司N成立於2009年，總部位於北京。該公司是一家私有專業數據安全產品與服務的提供商。

中國數據安全供應商排名(按專業安全供應商劃分)

2025年中國數據安全專業安全供應商細分市場競爭格局激烈，前十大供應商合計佔據60.9%的市場份額，其中公司A、公司D、公司E及本公司等企業處於領先地位。

作為專業安全供應商，本公司在中國數據安全專業安全供應商細分市場中位列第七，市場份額為3.8%。這彰顯了其技術實力與市場洞察力，表明在不斷發展的數據安全領域中，該公司擁有巨大的增長潛力。

中國數據安全市場正蓬勃發展，這得益於嚴格法規(如《數據安全法》)的推動、數字經濟的擴張，以及對數據治理、合規性與隱私保護日益增長的需求。

排名	公司	市場份額(按收入計)
1	公司A	13.4%
2	公司D	8.3%
3	公司E	7.7%
4	公司C	6.5%
5	公司G	6.2%
6	公司K	5.0%
7	本公司	3.8%
8	公司B	3.6%
9	公司I	3.2%
10	公司N	3.2%
其他		39.1%
總計		100%

圖 11. 2025 年數據安全供應商收入排名前 10 位(中國，按專業安全供應商劃分)

資料來源：弗若斯特沙利文；各市場參與者的年報；行業專家訪談

行業概覽

中國數據安全平台供應商排名(按專業安全供應商劃分)

中國數據安全行業中的數據安全平台市場代表了一個關鍵的增長領域，市場規模為人民幣15億元(2025年)。該細分領域以集中化治理解決方案需求加速增長為特徵，致力於滿足不斷演變的合規要求(如DSL、PIPL)以及混合雲數據保護需求。關鍵驅動因素包括電信、政府、能源電力、金融及製造行業採用率的提升。平台能力—尤其是大數據吞吐量、人工智能驅動的預警、動態監控、自動化策略執行和基於API的集成能力—正逐漸成為決定性的競爭差異化因素。企業投資優先級現已轉向統一控制平面，相較於點解決方案，其能顯著降低營運成本。

2025年，數據安全平台市場顯示出一定程度的集中，前10大供應商佔據56.9%的市場份額，表明市場仍有顯著的剩餘空間。

本公司以9.7%的市場份額位居上榜廠商榜首，領先於主要競爭對手，如公司G(8.3%)、公司A(7.2%)和公司O(5.6%)等。其領導地位體現了在安全平台架構和行業定制化方面的強大定位。

排名	公司	市場份額(按收入計)
1	本公司	9.7%
2	公司G	8.3%
3	公司A	7.2%
4	公司O	5.6%
5	公司E	5.5%
6	公司N	5.2%
7	公司D	4.3%
8	公司B	4.1%
9	公司M	3.8%
10	公司C	3.3%
其他		43.1%
總計		100%

圖 12. 2025年數據安全平台供應商收入排名前10位(中國，按專業安全供應商劃分)

資料來源：弗若斯特沙利文；各市場參與者的年報；行業專家訪談

附註：公司O成立於2005年，總部位於杭州，是一家私有數據安全及數字化轉型產品及服務提供商。

中國網絡安全供應商排名(按專業安全供應商劃分)

2025年，按收入計，中國網絡安全專業安全供應商細分市場的市場規模達到人民幣312億元。公司B、公司A及公司F等公司在市場中佔據重要地位，前15大網絡安全供應商合計佔整體市場的65.1%。

本公司以1.1%的市場份額排名第14位，為迅速崛起的新興競爭者。在技術進步及對數字化防護需求上升的驅動下，中國網絡安全市場競爭激烈且演變迅速。關鍵競爭因素包括解決方案的全面性、可擴展性、安全穩健性及品牌聲譽。本公司憑藉其專業的網絡安全產品及客戶網絡實現顯著增長，展現出強大的市場競爭力。

行業概覽

排名	公司	市場份額(按收入計)
1	公司B	10.4%
2	公司A	8.0%
3	公司F	6.9%
4	公司C	6.6%
5	公司D	6.0%
6	公司E	5.5%
7	公司G	5.3%
8	公司H	3.8%
9	公司I	3.1%
10	公司J	2.6%
11	公司L	2.0%
12	公司K	1.4%
13	公司M	1.2%
14	本公司	1.1%
15	公司P	1.1%
其他		34.9%
總計		100%

圖 13. 2025 年網絡安全供應商收入排名前 15 位(中國，按專業安全供應商劃分)

資料來源：弗若斯特沙利文；各市場參與者的年報；行業專家訪談

附註：公司P成立於2005年，總部位於北京。該公司是一家專注於數據安全、公共安全及雲安全的私有信息安全技術企業。

中國網絡安全平台供應商排名(按專業安全供應商劃分)

前15大領先供應商(包括公司A、公司F、公司B、公司G及公司E)持有超過64.4%的市場份額。其中，公司A以9.4%的份額位居首位，其後依次為公司F、公司B及公司G。

本公司與公司H均持有1.5%的市場份額。本集團將人工智能及大數據建模算法應用於網絡安全，在網絡安全平台市場中極具競爭力。

排名	公司	市場份額(按收入計)
1	公司A	9.4%
2	公司F	9.2%
3	公司B	8.9%
4	公司G	6.2%
5	公司E	6.1%
6	公司D	6.1%
7	公司C	4.2%
8	公司I	3.6%
9	公司M	2.2%
10	公司H	2.0%
11	本公司	1.5%
12	公司P	1.4%
13	公司N	1.3%
14	公司Q	1.2%
15	公司K	1.1%
其他		35.6%
總計		100%

圖 14. 2025 年網絡安全平台供應商收入排名前 15 位(中國，按專業安全供應商劃分)

資料來源：弗若斯特沙利文；各市場參與者的年報；行業專家訪談

附註：公司Q成立於1999年，總部位於廈門，於2011年在深圳證券交易所上市。該公司專注於電子數據取證、公共安全大數據、新型網絡空間安全及數字政府服務。

行業概覽

資料來源

本公司已委託獨立市場研究及諮詢公司弗若斯特沙利文對中國的信息安全市場、中國的數據安全市場、中國的網絡安全市場進行分析及編製報告。弗若斯特沙利文為本公司編製的報告在本文件內指弗若斯特沙利文報告。本公司向弗若斯特沙利文支付人民幣568,000元的費用，本公司認為該費用反映了此類報告的市場價格。

弗若斯特沙利文成立於1961年，在全球設有40個辦事處，擁有逾2,000名行業顧問、市場研究分析員、技術分析員及經濟學家。弗若斯特沙利文的服務涵蓋技術研究、獨立市場研究、經濟研究、企業最佳常規諮詢、培訓、客戶研究、競爭情報及企業策略。

弗若斯特沙利文報告包括中國信息安全市場、中國數據安全市場、中國網絡安全市場的資料以及其他經濟數據，且已在本文件中載列。弗若斯特沙利文的獨立研究包括從各種來源獲得的有關目標市場的一手及二手資料。一手研究包括與主要行業參與者及行業專家進行深入訪談。二手研究包括查閱公司報告、獨立研究報告及基於弗若斯特沙利文自身研究數據庫的數據。預測數據自過往數據分析得出，並與宏觀經濟數據比較，當中參考特定行業相關因素。除另有註明者外，本節所載全部數據及預測摘錄自弗若斯特沙利文報告、各政府官方刊物及其他刊物。

於編撰及編製弗若斯特沙利文報告時，弗若斯特沙利文曾採用下列假設：(i)未來十年，中國的經濟很有可能維持穩定增長及(ii)中國社會、經濟及政治環境在預測期內可能保持穩定，從而確保中國信息安全市場、中國數據安全市場、中國網絡安全市場穩定健康發展。